The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

DATE(S) ISSUED:

09/10/2013

SUBJECT:

Vulnerability in Microsoft Outlook Could Allow Remote Code Execution (MS13-068)

OVERVIEW:

A vulnerability has been identified in Microsoft Outlook which could allow for remote code execution. Microsoft Outlook is an email client. Successful exploitation of the vulnerability could allow an attacker to gain the same privileges as the local user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

SYSTEMS AFFECTED:

- Microsoft Office 2007
- Microsoft Office 2010

RISK:

Government:

- Large and medium government entities: **High**
- Small government entities: **High**

Businesses:

- Large and medium business entities: **High**
- Small business entities: **High**

Home users: High

DESCRIPTION:

A vulnerability has been identified in Microsoft Outlook which could allow for remote code execution. This vulnerability is caused when Microsoft Outlook fails to properly parse the contents of a Secure/Multipurpose Internet Mail Extension (S/MIME) message. S/MIME is used to provide a consistent way to send and receive MIME encoded data securely. An attacker could exploit this vulnerability by sending a specially crafted email message to the user, and then convincing the user to preview or open the email. Successful exploitation of the vulnerability could allow an attacker to gain the same privileges as the local user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

RECOMMENDATIONS:

The following actions should be taken:

- Apply appropriate patches provided by Microsoft to vulnerable systems immediately after appropriate testing.
- Remind users not to open e-mail attachments from unknown users or suspicious e-mails from trusted sources.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.

REFERENCES:

Microsoft:

https://technet.microsoft.com/en-us/security/bulletin/ms13-068

CVE:

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-3870